JP-A-H7-182112 discloses:

Purpose: To provide a data processor which contains a secret protecting function of writing data to a replaceable storage medium to enable even another processor to read the file data out of the storage medium.

Constitution: A data processor is provided with a coding means which codes the file management data recorded on a replaceable storage medium, and a decoding means which decodes the coded data. Then a reading/writing means is added to write or read the uncoded data into or out of the medium. Thus the data decoded by the means are recorded on the medium by the means. When a user approves to read the file data by another data processor, the data coded in the medium are decoded. Then the coded data that can be read by another data processor are recorded on the medium by the means.

The data are encoded using a value randomly written, with respect to a byte, based on a encoding table.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－182112

(43)公開日　平成７年(1995)７月21日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	3/06	３０４　Ｈ			
Ｇ１１Ｂ	20/10	Ｈ	7736－5Ｄ		
	20/12		9295－5Ｄ		

審査請求　未請求　請求項の数６　ＦＤ　（全８頁）

(21)出願番号　　願平5－346049

(22)出願日　　平成５年(1993)12月24日

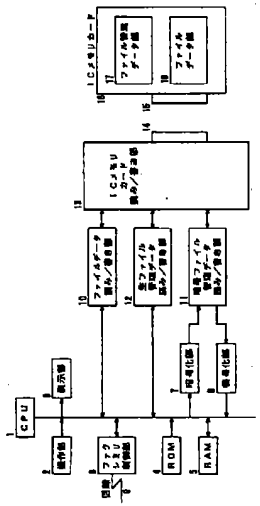
(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72)発明者　豊田　清
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　弁理士　役　昌明　（外１名）

(54)【発明の名称】機密保護機能を持つデータ処理装置

(57)【要約】
【目的】　他の装置でも可換記憶媒体のファイルデータの読出しができるように可換記憶媒体への書込みを行なう機密保護機能を備えたデータ処理装置を提供する。
【構成】　可換記憶媒体16に記録するファイル管理データ17の暗号化手段７と、暗号化されたファイル管理データの復号化手段８とを備えるデータ処理装置において、暗号化されていないファイル管理データを可換記憶媒体16に書込みまたは読出す読み／書き手段12を設け、復号化手段８で復号化したファイル管理データを読み／書き手段12で可換記憶媒体16に記録する。ユーザが、他のデータ処理装置でファイルデータを読むことを認める場合は、可換記憶媒体16の暗号化されたファイル管理データが復号された後、読み／書き手段12を通じて、この復号されて他の装置でも読める状態のファイル管理データが可換記憶媒体16に記録される。



1

【特許請求の範囲】
【請求項１】　可換記憶媒体に記録するファイル管理データを暗号化する暗号化手段と、暗号化された前記ファイル管理データを復号化する復号化手段とを備える、機密保護機能を持つデータ処理装置において、
暗号化されていない前記ファイル管理データを前記可換記憶媒体に書込みまたは読出す読み／書き手段を設け、前記復号化手段によって復号化された前記ファイル管理データを前記読み／書き手段により前記可換記憶媒体に記録できるように構成したことを特徴とするデータ処理装置。
【請求項２】　パスワードを入力する入力手段を設け、前記パスワードが入力されたときに、前記読み／書き手段が復号化された前記ファイル管理データを前記可換記憶媒体に記録するように構成したことを特徴とする請求項１に記載のデータ処理装置。
【請求項３】　前記可換記憶媒体が装着されたことを検知する検知手段を設け、前記検知手段の検知に応じて、前記暗号化手段を起動し、暗号化された前記ファイル管理データを前記可換記憶媒体に記憶させることを特徴とする請求項１または２に記載のデータ処理装置。
【請求項４】　前記暗号化手段が、暗号化テーブルと、前記暗号化テーブルに書込まれた値と前記ファイル管理データの値とを演算して暗号化されたファイル管理データの値を生成する演算手段とを備えることを特徴とする請求項１乃至３に記載のデータ処理装置。
【請求項５】　前記暗号化テーブルが、各バイト毎に書込まれたランダムな値を有し、前記演算手段が、前記ファイル管理データの各バイト毎の値の大きさに応じて、該ファイル管理データの値と前記暗号化テーブルの値とを加算または減算し、前記加算または減算の別を前記暗号化テーブルに残すことを特徴とする請求項４に記載のデータ処理装置。
【請求項６】　前記暗号化手段が、前記可換記憶媒体へのファイル管理データの書込み位置をずらす手段によって構成されることを特徴とする請求項１に記載のデータ処理装置。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、作成したファイルデータをフロッピディスクやＩＣメモリカード等の可換記憶媒体に保存するデータ処理装置に関し、特に、可換記憶媒体に記憶されたファイルデータの機密を保持すると共にデータ交換の便をも与えることができるように構成したものである。
【０００２】
【従来の技術】情報化時代の昨今では、パーソナルコンピュータ等のデータ処理装置を用いて個人用のファイルを作成し、管理することが広く行なわれている。これらの装置では、ファイルの保存や他の装置へのデータ交換

2

にフロッピディスクやＩＣメモリカード等の可換記憶媒体が使用される。可換記憶媒体は、誰でも簡単に装置から取外すことができ、データ交換が非常に便利である。しかし、これは、逆に言えば、知られたくないデータが他人に簡単に漏れてしまう可能性も高く、そのため、可換記憶媒体に記録された個々人のデータの機密保護を如何に行なうかということが重要な問題になっている。
【０００３】従来、可換記憶媒体に記憶されたファイルデータの機密を守るために、可換記憶媒体にファイルデータとは別のパスワードファイルを付加し、ユーザが入力したパスワードを照合して、一致したときのみにファイルの読出しを許可し、パスワードが一致しなければファイルデータを読み出すことができないように構成していた。しかし、この方法では、データ交換先のデータ処理装置がパスワードの照合機能を持たない構造の場合には、可換記憶媒体のファイルデータが読出されてしまう。
【０００４】こうした点を改善するため、特開平４－１６３７６８号公報には、可換記憶媒体に記憶されるファイル管理データを暗号化することによって、機密保護を図ることが提案されている。
【０００５】この可換記憶媒体を扱うデータ処理装置は、図９に示すように、ディスクカートリッジ43（可換記憶媒体）のファイル管理データ44およびファイルデータ45の読出しまたは書込みを行なうディスク読み／書き部42と、ファイルデータの読出しまたは書込みを行なうファイルデータ読み／書き部40と、暗号化されたファイル管理データの読出しまたは書込みを行なう暗号ファイル管理データ読み／書き部41と、ファイル管理データの暗号化に使用される暗号化キーを記憶する暗号化キーレジスタ36と、この暗号化キーを用いてディスク43に書込むファイル管理データを暗号化する暗号化部37と、暗号化されたファイル管理データを解読するための復号化キーを記憶する復号化キーレジスタ39と、この復号化キーを用いてファイル管理データを解読し平文に変換する復号化部38と、操作者が暗号化キーおよび復号化キーを入力する操作部32と、この装置の動作を総合的に制御するＣＰＵ31と、ＣＰＵ31の実行する制御プログラムが格納されたＲＯＭ34と、ＣＰＵ31のワーク領域として機能するＲＡＭ35と、所要の表示を行なう表示部33とを備えている。
【０００６】ファイル管理データには、ファイル名、ファイルのサイズ、ロケーション（記憶場所）等が含まれ、また、機密保護をさらに確実にするためにファイルデータを変換キーで変換して記録する場合には、その変換キーも管理データの内に含まれる。こうしたファイル管理データが分からなければ、可換記憶媒体に正しくアクセスすることができないため、可換記憶媒体に記憶されたファイルデータの読出しが不可能になる。
【０００７】この装置を使って、装着したディスクカー

使用後返却願います

トリッジ43にデータを記録する場合には、操作者は、操作部32から暗号化キーを入力する。この暗号化キーは、暗号化キーレジスタ36に記録される。

【０００８】ファイルデータは、ファイルデータ読み／書き部40およびディスク読み／書き部42を介して、ディスクカートリッジ43のファイルデータ部45に書込まれる。また、ファイル管理データは、暗号化部37において、暗号化キーレジスタ36に記録された暗号化キーを用いて暗号化され、暗号ファイル管理データ読み／書き部41およびディスク読み／書き部42を介して、ディスクカートリッジ43のファイル管理データ部44に書込まれる。

【０００９】一方、このディスクカートリッジ43を装着してファイルデータを読出す場合には、操作者は、操作部32から復号化キーを入力する。この復号化キーは、復号化キーレジスタ39に記録される。

【００１０】ディスクカートリッジ43のファイル管理データ部44に記録されている暗号化されたファイル管理データは、ディスク読み／書き部42および暗号ファイル管理データ読み／書き部41を介して読出され、復号化部38は、この暗号化されたファイル管理データを、復号化キーレジスタ39に記録された復号キーを用いて解読し、平文のファイル管理データに変換して、ＲＡＭ35に格納する。

【００１１】ＣＰＵ31は、ＲＡＭ35に格納されたファイル管理データからアクセスすべきファイルのファイル名、サイズ、ロケーション等の情報を読取り、それを基にデータ読出しの動作を制御する。その結果、ディスクカートリッジ43のファイルデータ部45に記録されたファイルデータは、ディスク読み／書き部42およびファイルデータ読み／書き部40を介して読取られる。

【００１２】このように、暗号化されたファイル管理データは、復号化キーを入力することによって復号化され、それによりファイルデータの読出しが可能になる。従って、復号化キーを知らない他人はファイルデータを読出すことができず、ファイルデータの機密が保護される。

【００１３】

【発明が解決しようとする課題】しかし、このように暗号化および復号化する機構を備えた従来のデータ処理装置で記録された可換記憶媒体のファイルデータは、同じ機構を備えた装置以外では読出すことができない。そのため、可換記憶媒体に記録されたファイルデータをデータ交換しようとする場合等には不便が生ずる。

【００１４】本発明は、こうした従来の問題点を解決するものであり、必要に応じて、同じ機密保護機能を持たない装置でも可換記憶媒体のファイルデータを読出すことができるように、可換記憶媒体への書込みを行なうことができる機密保護機能を備えたデータ処理装置を提供することを目的としている。

【００１５】

【課題を解決するための手段】そこで、本発明では、可換記憶媒体に記録するファイル管理データを暗号化する暗号化手段と、暗号化されたファイル管理データを復号化する復号化手段とを備える機密保護機能を持つデータ処理装置において、暗号化されていないファイル管理データを可換記憶媒体に書込みまたは読出す読み／書き手段を設け、復号化手段によって復号化されたファイル管理データをこの読み／書き手段により可換記憶媒体に記録できるように構成している。

【００１６】また、パスワードを入力する入力手段を設け、パスワードが入力されたときに、読み／書き手段が復号化されたファイル管理データを可換記憶媒体に記録するように構成している。

【００１７】また、可換記憶媒体が装着されたことを検知する検知手段を設け、この検知手段の検知に応じて、暗号化手段を起動し、暗号化されたファイル管理データを可換記憶媒体に記憶させるように構成している。

【００１８】また、暗号化手段を、暗号化テーブルと、この暗号化テーブルに書込まれた値とファイル管理データの値とを演算して、暗号化されたファイル管理データの値を生成する演算手段とで構成している。

【００１９】また、この暗号化テーブルが、各バイト毎に書込まれたランダムな値を有し、演算手段が、ファイル管理データの各バイト毎の値の大きさに応じて、このファイル管理データの値と暗号化テーブルの値とを加算または減算し、この加算または減算の別を暗号化テーブルに残すように構成している。

【００２０】さらに、暗号化手段を、可換記憶媒体へのファイル管理データの書込み位置をずらす手段によって構成している。

【００２１】

【作用】そのため、ユーザが、可換記憶媒体に記録されたファイルデータを機密保護機能を持たない他のデータ処理装置で読出すことを認める場合には、可換記憶媒体の暗号化されているファイル管理データが、復号化手段によって復号された後、読み／書き手段を通じて可換記憶媒体に記録される。従って、可換記憶媒体は、暗号化されていないファイル管理データを持つことになり、このファイル管理データは他の装置でも読むことが可能になる。

【００２２】このファイル管理データの非暗号化は、機密保護の観点から、ユーザがパスワードを入力したときに実行される。

【００２３】可換記憶媒体の装着を検知する検知手段を設けた場合には、暗号化の指令を入力しなくとも、装着した可換記憶媒体のファイル管理データに対する暗号化が自動的に行なわれる。

【００２４】また、暗号化テーブルと演算処理手段とによってファイル管理データの暗号化を行なうことにより、特別な暗号化の回路が不要になり、構成を簡素化することができる。

【００２５】さらに、ファイル管理データの記録位置をずらすことによっても、他の装置ではファイル管理データが読めなくなり、暗号化の効果を上げることができる。この場合、復号時には、記録時にずらした位置からファイル管理データを読出すことにより、元のファイル管理データを復元できる。

【００２６】

【実施例】

（第１実施例）本発明の第１実施例のデータ処理装置は、図１に示すように、可換記憶媒体として、ファイル管理データ部17とファイルデータ部18とを具備するＩＣメモリカード16を使用している。ＩＣメモリカード16は、またインタフェース15を有している。装置本体は、インタフェース14を通じてＩＣメモリカード16との間でファイル管理データおよびファイルデータの読出しまたは書込みを行なうＩＣメモリカード読み／書き部13と、ファイルデータの読出しまたは書込みを行なうファイルデータ読み／書き部10と、暗号化されたファイル管理データの読出しまたは書込みを行なう暗号ファイル管理データ読み／書き部11と、暗号化されていない生ファイル管理データの読出しまたは書込みを行なう生ファイル管理データ読み／書き部12と、ＩＣメモリカード16に書込むファイル管理データを暗号化する暗号化部７と、暗号ファイル管理データを解読して生ファイル管理データに変換する復号化部８と、操作者が指示を入力する操作部２と、この装置の動作を総合的に制御するＣＰＵ１と、ＣＰＵ１の実行する制御プログラムが格納されたＲＯＭ４と、読出された生ファイル管理データが一時格納されるＲＡＭ５と、回線９を通じてファクシミリデータを送受信するファクシミリ制御部６と、所要の表示を行なう表示部３とを備えている。

【００２７】この装置は、暗号化されたファイル管理データを有するＩＣメモリカード16からファイルデータを読出したり、書込んだりすることができ、また、ＩＣメモリカードの暗号化されていないファイル管理データを暗号化することができ、その逆に、暗号化されているファイル管理データを暗号化されていないファイル管理データに変換することができる。

【００２８】ＩＣメモリカード16のファイル管理データが暗号化されている場合には、復号方法を知る操作者が、この機密保護機能を備えた装置を使ってファイルデータを読出す以外に、それを読出すことができない。このファイル管理データを暗号化されていないファイル管理データに変換した場合には、他の装置によりファイルデータを読出すことが可能になる。

【００２９】この装置を用いて、いずれの操作をする場合にも、まず、装着したＩＣメモリカード16のファイル管理データを読取ることが必要になる。このファイル管理データには、図２に例示するように、ファイル管理データが暗号化されているか否かを示す暗号化フラグ、各ファイルに対応するファイル名、カード上の記録位置、ファイルの長さ、記録の日付およびファイルの属性等が含まれる。

【００３０】装着したＩＣメモリカード16のファイル管理データが暗号化されていない場合（暗号化フラグが非暗号化を示している場合）には、生ファイル管理データ読み／書き部12が、ＩＣメモリカード読み／書き部13を介して、ＩＣメモリカード16のファイル管理データを読出し、ＲＡＭ５に書込む。また、暗号化されている場合（暗号化フラグが暗号化を示している場合）には、暗号化ファイル管理データ読み／書き部11が、ＩＣメモリカード読み／書き部13を介して、ＩＣメモリカード16のファイル管理データを読出し、復号化部８がこれを解読して生ファイル管理データに変換し、ＲＡＭ５に書込む。

【００３１】ＣＰＵ１は、ＲＡＭ５に格納されたファイル管理データからアクセスすべきファイルを識別し、データ読出しまたは書込みの動作を制御する。例えば、読出しの場合には、ＣＰＵ１の制御を受けたファイルデータ読み／書き部10が、ＩＣメモリカード16のファイルデータ部18に記録されたファイルデータを、ＩＣメモリカード読み／書き部13を介して読取り、ファクシミリ制御部６を通じて回線９に送信する。

【００３２】また、この装置を用いて、ＩＣメモリカードの暗号化されていないファイル管理データを暗号化する場合には、このＩＣメモリカードのファイル管理データを生ファイル管理データ読み／書き部12が読出してＲＡＭ５に書込み、次いで暗号化部７がＲＡＭ５に書込まれたファイル管理データを読出して暗号化し、この暗号化したファイル管理データを、暗号ファイル管理データ読み／書き部11が、ＩＣメモリカード読み／書き部13を介して、ＩＣメモリカード16のファイル管理データ部17に書込む。この場合、暗号化は、ファイル管理データの少なくともファイル名および記憶位置のデータについて行なわれる。

【００３３】また、ＩＣメモリカードの暗号化されたファイル管理データを暗号化されていないファイル管理データに変換する場合は、ＩＣメモリカードのファイル管理データを暗号ファイル管理データ読み／書き部11が読出し、復号化部８が生ファイル管理データに変換してＲＡＭ５に書込み、次いで生ファイル管理データ読み／書き部12がＲＡＭ５に書込まれたファイル管理データを読出し、ＩＣメモリカード読み／書き部13を介して、ＩＣメモリカード16のファイル管理データ部17に書込む。この動作は、操作者が操作部２からパスワードを入力した場合に限って行なわれる。

【００３４】ここで、ＩＣメモリカードの生ファイル管理データを暗号化し、ＩＣメモリカードにファイルデータを書込み、次いで、他の装置による読出しを可能にするためにＩＣメモリカードの機密化を解除するまでの一

7

連の手順を図３のフローチャートに基づいて説明する。

【００３５】ステップ１；操作者は、データ処理装置にＩＣメモリカード16を装着し、

ステップ２；操作部２より、暗号化の指示を入力する。

【００３６】ステップ３；ＣＰＵ１は、この指示を受けて、ＩＣメモリカード16のファイル管理データの読込みを指令し、生ファイル管理データ読み／書き部12は、ＩＣメモリカード読み／書き部13を介して、ＩＣメモリカード16のファイル管理データを読込み、ＲＡＭ５に書込む。

【００３７】ステップ４；暗号化部７は、ＣＰＵ１の指令を受けて、ＲＡＭ５に書込まれた生ファイル管理データの少なくともファイル名および記憶位置のデータを暗号化する。この暗号化されたファイル管理データは、暗号ファイル管理データ読み／書き部11およびＩＣメモリカード読み／書き部13を介して、ＩＣメモリカード16のファイル管理データ部17に書込まれる。こうしてＩＣメモリカードの生ファイル管理データの暗号化が終了する。

【００３８】ステップ５；ファイルデータの書込みは、ＣＰＵ１の指令に従ってファイルデータ読み／書き部10が実行し、ファクシミリ制御部６を通じて受信した回線９からのデータを、ＩＣメモリカード読み／書き部13を介して、ＩＣメモリカード16のファイルデータ部18に記録する。このファイルデータの書込みに伴って、ＲＡＭ５に記憶されたファイル管理データの内容が変更され、変更後のファイル管理データは、暗号化部７で暗号化された後、暗号ファイル管理データ読み／書き部11から、ＩＣメモリカード読み／書き部13を介して、ＩＣメモリカード16のファイル管理データ部17に送られ、ファイル管理データを更新する。こうしてＩＣメモリカードへのファイルデータの書込みが終了する。

【００３９】ステップ６；操作者は、ＩＣメモリカード16に記録されたファイルデータを、機密保護機能を持たない他の装置でも読出せるようにしたいときは、操作部２からパスワードを入力する。

【００４０】ステップ７；パスワードが入力されると、ＩＣメモリカード16の暗号化されたファイル管理データは、暗号ファイル管理データ読み／書き部11に読出され、復号化部８で生ファイル管理データに変換された後、ＲＡＭ５に格納される。次いでこのファイル管理データは、生ファイル管理データ読み／書き部12に読出され、ＩＣメモリカード16のファイル管理データ部17に格納される。

【００４１】ステップ８；この格納が終了すると、表示部３は、ＩＣカードを装置から抜いても良い状態にあることをユーザに表示し、ユーザはこれを確認してＩＣメモリカードを抜く。

【００４２】このようにＩＣメモリカード16の機密化の解除は、操作者がパスワードを入力すると、装置が自動的に実行する。

8

【００４３】（第２実施例）第２実施例のデータ処理装置では、ＩＣメモリカードを挿入すると、操作者が暗号化の指令を入力しなくても、自動的にＩＣメモリカードのファイル管理データが暗号化される。この装置は、図４に示すように、ＩＣメモリカード読み／書き部13にＩＣメモリカードの装着を検出するカード挿入検知部19を備えている。その他の構成は、第１実施例の装置（図１）と変わりがない。

【００４４】この装置では、操作者がＩＣメモリカード16を挿入すると、カード挿入検知部19を通じてそれを検知したＣＰＵ１が、ＩＣメモリカード16のファイル管理データの暗号化を指令し、図３におけるステップ３以降の動作が実行される。

【００４５】なお、ＩＣメモリカードが挿入された後、初めてファイルアクセスが行なわれた時期を自動検知するように構成し、この自動検知の時期に合わせて暗号化を実施させることも可能である。

【００４６】（第３実施例）第３実施例のデータ処理装置は、ファイル管理データの暗号化を、暗号化回路を用いずに、簡単な方式によって実施している。この装置は、図５に示すように、ファイル管理データの暗号化に使用する暗号化テーブル21と、暗号化の演算を実行する演算処理部20とを備えている。その他の構成は第１実施例の装置（図１）と変わりがない。

【００４７】暗号化テーブル21は、１バイト毎に１～１２７のランダムな値が収められており、演算処理部20は、この暗号化テーブル21を使って、図６に示す手順でファイル管理データを暗号化する。

【００４８】ステップ３１；暗号化テーブル21の１バイト毎の値と、ファイル管理データの１バイト毎の値とを比較する。

【００４９】ステップ３２；ファイル管理データの値が０～１２７の範囲にあるかどうかを見て、

ステップ３３；ファイル管理データの値が０～１２７のときは、このデータの値から暗号化テーブルの値を減算し、その結果、得られた値をファイル管理データの値とする。

ステップ３４；また、ファイル管理データの値が－１２７～－１のときは、このデータの値と暗号化テーブルの値とを加算し、その結果、得られた値をファイル管理データの値とする。

【００５０】ステップ３５；加算したときは暗号化テーブル21の該当する数値にマイナス符号をつけて暗号化テーブル21を更新する。

【００５１】ステップ３６；こうした処理をファイル管理データの暗号化すべき項目について繰り返し実施する。

【００５２】一方、復号化するときは、暗号化テーブル21の値とファイル管理データの値とを各バイト毎に加算する。こうすることにより基のファイル管理データの値が求められる。復号化の演算後は、暗号化テーブルの数値に付けたマイナス符号を取り除く。

9

【００５３】（第４実施例）第４実施例のデータ処理装置は、ファイル管理データをＩＣメモリカードのファイル管理データ部17に位置をずらして書込むことにより、暗号化と同じ効果を上げている。この装置は、図７に示すように、ファイル管理データ部17にファイル管理データを位置をずらして書込みまたは読出すことができるファイル管理データ位置制御部22を備えている。その他の構成は第１実施例の装置（図１）と変わりがない。

【００５４】この装置では、図３のステップ４における暗号化に際して、図８（ａ）に示すように、

ステップ４１；ファイル管理データ位置制御部22は、ファイル管理データをＩＣメモリカード16のファイル管理データ部17に、位置をずらして書き込む。こうすることによりＩＣメモリカード16は、本装置以外で読めなくなる。

【００５５】また、このＩＣメモリカード16を他の装置でも読出せるように、操作者が操作部２からパスワードを入力した場合には、図８（ｂ）に示すように、

ステップ４２；ファイル管理データ位置制御部22は、ファイル管理データ部17のずれた位置（書込み時にずらした位置）からファイル管理データを読込んでＲＡＭ５に書込み、

ステップ４３；生ファイル管理データ読み／書き部12は、このＲＡＭ５のファイル管理データを読出し、ＩＣメモリカード16のファイル管理データ部17の正規の位置にこのファイル管理データを書込む。

【００５６】このように、第４実施例の装置では、暗号化回路を使わずに、簡単な構成でＩＣメモリカードの機密保護を実現している。

【００５７】なお、各実施例では、可換記憶媒体としてＩＣメモリカードを用いているが、フロッピディスク等、他の装着・着脱の可能な記憶媒体を用いることも勿論可能である。

【００５８】また、先に示した従来のデータ処理装置と同じように、ファイルデータを変換キーによって変換して可換記憶媒体に書込むと共に、この変換キーをファイル管理データの中に含めて暗号化することも可能である。

【００５９】

【発明の効果】以上の実施例の説明から明らかなように、本発明のデータ処理装置は、可換記憶媒体に記憶されたファイルデータの機密を厚く保護することができる。また、ユーザが許す場合には、可換記憶媒体に記憶されたファイルデータを機密保護機能を持たないデータ処理装置で読出せるように変換することができる。この変換は、ユーザがこの装置にパスワードを入力することにより自動的に実行される。従って、ユーザ自身は、変換のためのロードを特に必要としない。一方、パスワードを知らない第三者は、この変換を行なうことができず、データの機密は保護される。

10

【００６０】また、暗号化テーブルと演算処理部とを用いることにより、特別な暗号化回路を使わずに、可換記憶媒体のファイルデータの機密を保護することができる。

【００６１】さらに、ファイル管理データをずらして書込むという簡便な手段によって、暗号化に相当する効果を得ることができる。

【図面の簡単な説明】

【図１】本発明の第１実施例におけるデータ処理装置の構成を示すブロック図、

【図２】前記データ処理装置で処理されるファイル管理データの内容を示す図、

【図３】第１実施例のデータ処理装置における動作手順を示すフローチャート、

【図４】本発明の第２実施例におけるデータ処理装置の構成を示すブロック図、

【図５】本発明の第３実施例におけるデータ処理装置の構成を示すブロック図、

【図６】第３実施例のデータ処理装置における動作手順を示すフローチャート、

【図７】本発明の第４実施例におけるデータ処理装置の構成を示すブロック図、

【図８】第４実施例のデータ処理装置における暗号化（ａ）および復号化（ｂ）の動作手順を示すフローチャート、

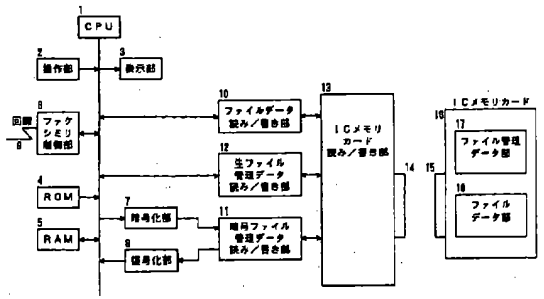
【図９】従来のデータ処理装置の構成を示すブロック図である。

【符号の説明】

１、31　ＣＰＵ
２、32　操作部
３、33　表示部
４、34　ＲＯＭ
５、35　ＲＡＭ
６　ファクシミリ制御部
７、37　暗号化部
８、38　複合化部
９　回線
10　ファイルデータ読み／書き部
11　暗号ファイル管理データ読み／書き部
12　生ファイル管理データ読み／書き部
13　ＩＣメモリカード読み／書き部
14　データ処理装置のインターフェイス部
15　ＩＣカードのインターフェイス部
16　ＩＣメモリカード
17　ファイル管理データ部
18　ファイルデータ部
19　カード挿入検知部

20　演算処理部
21　暗号化テーブル
22　ファイル管理データ部位置制御部
36　暗号化キーレジスタ
39　復号化キーレジスタ
40　ディスクカートリッジのファイルデータ読み／書き部
41　ディスクカートリッジの暗号ファイル管理データ部読み／書き部
42　ディスク読み／書き部
43　ディスクカートリッジ
44　ディスクカートリッジのファイル管理データ部
45　ディスクカートリッジのファイルデータ部

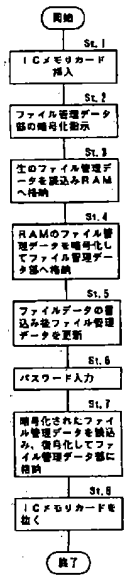
【図１】



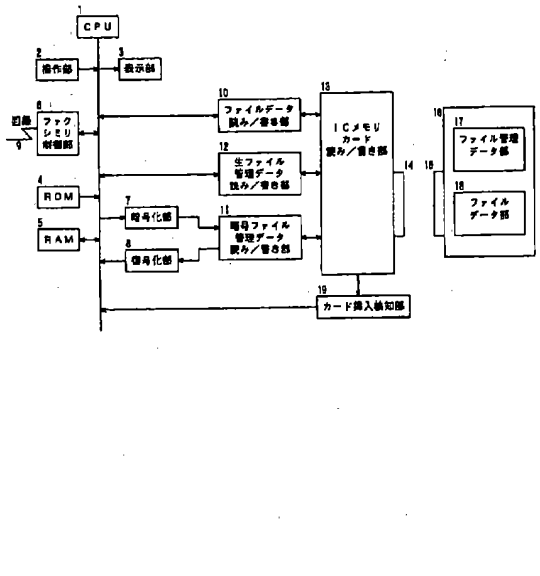
【図２】

暗号化フラグ				
ファイル名１	位置１	長さ１	日付１	属性１
ファイル名２	位置２	長さ２	日付２	属性２
・	・	・	・	・
・	・	・	・	・
・	・	・	・	・
ファイル名ｎ	位置ｎ	長さｎ	日付ｎ	属性ｎ

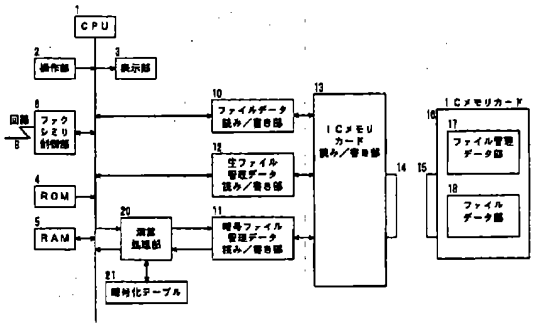
【図３】



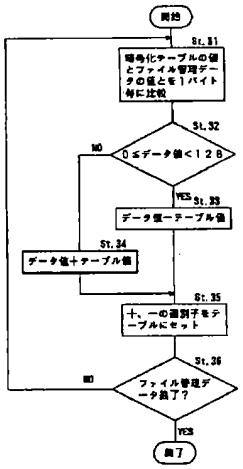
【図４】



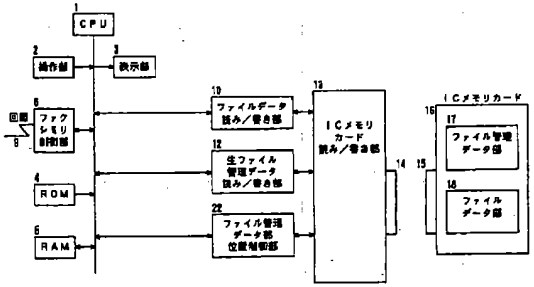
【図５】



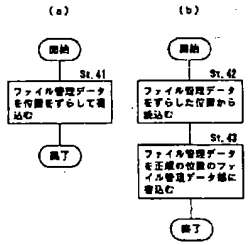
【図６】



【図７】



【図８】



【図９】